CARTILHA DE SEGURANÇA DIGITAL

Não Caia Nessa!

APRENDA A IDENTIFICAR GOLPES VIRTUAIS

Um guia prático para reconhecer, evitar e agir diante dos golpes por telefone, mensagem e internet.



Edição 2026

APRESENTAÇÃO

Golpe não escolhe idade nem escolaridade.

Todos os dias, milhares de pessoas recebem ligações, mensagens e links preparados para enganar. Os golpistas usam pressa, medo e confiança para fazer você agir antes de pensar.

Esta cartilha mostra, em linguagem simples, como esses golpes funcionam, quais sinais acendem o alerta e o que fazer para se proteger, e também o que fazer se o pior acontecer. Leia, guarde e compartilhe com quem você ama, principalmente com as pessoas mais velhas da família.

NESTA CARTILHA

1 **Por que falar de golpes** 3

2 **Como o golpista age** 4

3 **Os golpes mais comuns** 5

4 **Sinais de alerta** 7

5 **Como se proteger no dia a dia** 8

6 **Caiu no golpe? Aja rápido** 9

7 **Contatos úteis e fontes** 10

O golpe virou o crime mais comum do país.

O estelionato (o famoso "171") cresceu muito com o celular e o Pix. Hoje, o golpe chega pela palma da mão, a qualquer hora, e muitas vítimas nem registram ocorrência.

2,26 mi

registros de estelionato no Brasil em 2025, somando golpes comuns e por meio eletrônico.

Anuário Brasileiro de Segurança Pública 2026 (FBSP)

+430%

de aumento nos registros de estelionato entre 2018 e 2025.

Anuário Brasileiro de Segurança Pública 2026 (FBSP)

26,3 mi

de brasileiros (15,8% da população com 16 anos ou mais) caíram em golpe ou perderam dinheiro pela internet ou celular em um ano.

Pesquisa FBSP, março de 2026

R$ 25,5 bi

perdidos com golpes envolvendo Pix e boletos falsos em 12 meses.

Datafolha / FBSP, agosto de 2024

Os números reais são maiores

Muitas pessoas sentem vergonha e não denunciam. Cair em golpe não é falta de inteligência: os criminosos são profissionais e mudam de truque o tempo todo. Por isso, informação é a melhor proteção.

02 · COMO O GOLPISTA AGE

Ele não invade o celular. Ele convence você.

A maioria dos golpes usa a **engenharia social**: uma conversa bem ensaiada para que a própria vítima entregue a senha, o código ou o dinheiro. Para isso, o golpista aperta sempre os mesmos botões emocionais.

Pressa

Não dá tempo de pensar nem de confirmar.

"Resolva agora ou perde."

Medo

Ameaça de bloqueio, multa, processo ou prisão.

"Sua conta foi invadida."

Ganância

Prêmio, desconto ou lucro fácil demais.

"Você ganhou R$ 5.000!"

Afeto

Finge ser filho, neto ou amigo em apuros.

"Mãe, troquei de número."

Autoridade

Se passa por banco, advogado, polícia ou governo.

"Aqui é da central do banco."

Para parecer verdadeiro, o golpista muitas vezes já sabe seu nome, CPF, endereço ou data de nascimento, obtidos em vazamentos de dados. **Saber seus dados não prova que a pessoa é de confiança.** Hoje também existem golpes com inteligência artificial, capazes de imitar a voz ou o rosto de alguém conhecido.

A REGRA DE OURO

Pare. Desligue. Confirme.

1. **Pare**
   Sentiu pressa ou medo? É o sinal para desacelerar.
2. **Desligue**
   Encerre a ligação ou a conversa. Não clique em nada.
3. **Confirme**
   Procure você o canal oficial ou a pessoa, por outro meio.

Conheça o roteiro antes que ele chegue.

Falsa central do banco

● LIGAÇÃO · SMS

COMO FUNCIONA

Alguém liga dizendo ser do seu banco, fala seu nome e avisa de uma compra suspeita. Pede senha, código, que você instale um aplicativo ou faça uma "transferência de teste" para proteger a conta.

Proteja-se: desligue. Espere alguns minutos, ou use outro aparelho, e ligue você para o número do verso do cartão. Banco não pede senha nem transferência.

"Troquei de número"

● MENSAGEM

COMO FUNCIONA

O golpista usa a foto e o nome de um parente ou amigo, diz que trocou de número e pede um Pix urgente. Em outros casos, a conta verdadeira da pessoa foi clonada.

Proteja-se: ligue para o número antigo ou peça uma chamada de vídeo. Ative a verificação em duas etapas no aplicativo de mensagens.

Link falso (phishing)

● SMS · E-MAIL

COMO FUNCIONA

Mensagens que imitam banco, Correios, loja ou órgão público pedem para "regularizar", "liberar a entrega" ou "evitar a suspensão". O link leva a um site falso que rouba senhas e dados. O INSS, por exemplo, não envia links por SMS.

Proteja-se: não clique. Abra o aplicativo oficial ou digite você mesmo o endereço do site.

Pix "errado"

● PIX

COMO FUNCIONA

Um valor cai na sua conta "por engano" e alguém pede que você devolva para outra chave. Depois, o golpista pede ao banco a devolução do Pix original e você perde o dinheiro duas vezes.

Proteja-se: confira o extrato e devolva somente pela função de devolução do próprio aplicativo, nunca com um novo Pix.

Novos truques, o mesmo objetivo.

Loja, leilão e oferta falsos

● SITE · REDES

COMO FUNCIONA

Sites e perfis com preços muito abaixo do mercado, leilões de veículos, sorteios e o tal "bug do Pix", que promete multiplicar o dinheiro. Você paga e nada chega.

Proteja-se: desconfie de preço bom demais, pesquise o CNPJ e as reclamações da loja. Não existe falha que multiplique dinheiro.

QR Code e boleto falsos

● PIX · BOLETO

COMO FUNCIONA

Boletos e QR Codes adulterados, enviados por mensagem, e-mail ou redes sociais, desviam o pagamento para a conta do golpista.

Proteja-se: antes de confirmar, confira o nome e o banco de quem vai receber. Na dúvida, digite a chave Pix você mesmo.

Falso advogado ou autoridade

● LIGAÇÃO · VÍDEO

COMO FUNCIONA

O golpista se passa por advogado, juiz ou servidor público, cita um processo real ou inventado e cobra "taxas" urgentes para liberar valores ou evitar punições. Pode até marcar uma "audiência" por vídeo.

Proteja-se: confirme no número oficial do escritório ou do tribunal. Advogados e juízes não cobram por mensagem ou telefone.

Voz e vídeo falsos (IA)

● LIGAÇÃO · VÍDEO

COMO FUNCIONA

Com inteligência artificial, criminosos imitam a voz ou o rosto de alguém conhecido, ou de famosos, para pedir dinheiro ou anunciar investimentos milagrosos.

Proteja-se: combine uma palavra-senha com a família e faça uma pergunta que só a pessoa saberia responder.

04 · SINAIS DE ALERTA

Desconfie quando a mensagem...

Golpes mudam de roupa, mas deixam sempre as mesmas pistas. Use esta lista antes de clicar, pagar ou responder.

- **Pede pressa:** “agora”, “hoje”, “última chance”.
- **Ameaça:** bloqueio, multa, processo ou prisão.
- **Promete ganho fácil** ou um prêmio que você nem disputou.
- **Pede senha, código** recebido por SMS, foto de documento ou selfie.
- **Pede Pix, depósito** ou “transferência de teste”.
- **Traz link, QR Code** ou arquivo que você não esperava.
- **Pede para instalar** um aplicativo no seu celular.
- **Vem de um “novo número”** ou de contato desconhecido.
- **Pede segredo:** “não conte para ninguém”.
- **Tem endereço estranho:** letras trocadas, erros ou link encurtado.

Um sinal já basta para parar

Não espere juntar vários. Se uma única pista aparecer, encerre a conversa e confirme pelo canal oficial antes de fazer qualquer coisa.

Lembre-se

Bancos e órgãos públicos não pedem senha, código de verificação ou transferência por telefone, SMS ou aplicativo de mensagens.

05 · COMO SE PROTEGER

Pequenos hábitos, grande proteção.

NÃO FAÇA

- Clicar em links recebidos por mensagem ou e-mail
- Passar códigos que chegam por SMS
- Fazer Pix com pressa ou sob pressão
- Informar senha por telefone
- Instalar aplicativos a pedido de desconhecidos
- Usar a mesma senha em vários serviços

FAÇA ASSIM

- Digite você mesmo o endereço do site
- Ligue para o número oficial (verso do cartão)
- Confirme com a pessoa por outro canal
- Confira nome e banco antes de pagar
- Baixe aplicativos só da loja oficial
- Converse sobre golpes com a família

Configure hoje mesmo

Verificação em duas etapas
Ative no aplicativo de mensagens, no e-mail, nas redes sociais e na conta gov.br.

Limites do Pix
Ajuste no app do banco limites menores, principalmente à noite.

Senhas fortes e diferentes
Uma para cada serviço. Nunca anote no celular nem compartilhe.

Registrato (Banco Central)
Consulte de graça contas, empréstimos e chaves Pix ligados ao seu CPF.

BC Protege+
Avise o sistema financeiro que você não autoriza abrir contas no seu nome.

Celular Seguro (gov.br)
Cadastre seu aparelho para bloquear bancos e serviços em caso de roubo.

Combine uma palavra-senha com a família

Escolha uma palavra que só vocês conhecem. Se alguém pedir dinheiro em nome de um parente, mesmo com a voz ou o rosto dele, peça a palavra antes de qualquer Pix.

Não sinta vergonha. Aja rápido.

1. **Avise seu banco imediatamente**
   Use o aplicativo ou o número oficial. Se pagou com Pix, use o **botão de contestação** do app para acionar o **MED** (Mecanismo Especial de Devolução). Bloqueie cartões, se for o caso.

2. **Registre um boletim de ocorrência**
   Em São Paulo, pode ser feito pela internet na **Delegacia Eletrônica**. Guarde prints de conversas, números, comprovantes e links.

3. **Troque suas senhas**
   Comece pelo banco, e-mail, gov.br e aplicativo de mensagens. Ative a verificação em duas etapas.

4. **Avise seus contatos**
   Se sua conta foi clonada, alerte família e amigos para não atenderem pedidos de dinheiro em seu nome.

5. **Verifique seu CPF**
   Consulte o **Registrato** para ver se abriram contas ou empréstimos em seu nome e ative o **BC Protege+**.

6. **Procure seus direitos**
   Se o banco não resolver, registre reclamação no **Procon** ou procure o Judiciário.

Sobre a devolução do Pix (MED)

O botão de contestação está nos aplicativos dos bancos desde outubro de 2025. O pedido pode ser feito em até **80 dias** após a transferência, e o valor fica bloqueado na conta do golpista durante a análise. A devolução depende de ainda haver dinheiro lá, por isso **cada minuto conta**.

07 · CONTATOS ÚTEIS

Guarde estes canais oficiais.

EMERGÊNCIA

190

Polícia Militar, para crimes em andamento ou ameaças.

DENÚNCIA ANÔNIMA (SP)

181

Disque Denúncia do Estado de São Paulo.

BOLETIM DE OCORRÊNCIA ON-LINE (SP)

delegaciaeletronica.policiacivil.sp.gov.br

Registro de estelionato e golpes pela internet.

SEU BANCO

Verso do cartão ou app oficial

Nunca use números enviados por mensagem ou e-mail.

INSS

135

Ou o aplicativo e o site Meu INSS. O INSS não envia links por SMS.

PROCON-SP

procon.sp.gov.br

Reclamações contra bancos e lojas.

BANCO CENTRAL

bcb.gov.br · Registrato e BC Protege+

Acesso com a conta gov.br (nível prata ou ouro).

CELULAR ROUBADO

Celular Seguro (gov.br)

Bloqueio de bancos e serviços ligados ao aparelho.

Fontes consultadas

1. Fórum Brasileiro de Segurança Pública. Anuário Brasileiro de Segurança Pública 2026, via Brasil 61 (28/07/2026).
2. Datafolha / FBSP. Pesquisa sobre golpes com Pix e boletos, via Finsiders Brasil (13/08/2024).
3. Febraban. Levantamento sobre golpes mais praticados, via Olhar Digital (13/04/2025).
4. Banco Central. Botão de contestação do Pix, via IstoÉ Dinheiro (01/10/2025); prazo de 80 dias do MED, via Jornal Opção (01/09/2026).
5. Banco Central. Orientações a vítimas de golpes com Pix, via Diário do Nordeste.
6. INSS. Alerta sobre o golpe da falsa prova de vida, via NSC Total.
7. OAB e especialistas. Golpe do falso advogado com IA, via Seu Crédito Digital (30/08/2025).
8. Sicredi. Como funciona o golpe da falsa central; ferramentas Registrato, BC Protege+ e Celular Seguro, via Bem Paraná.
9. Procon-SP e Polícia Civil de SP: canais oficiais de atendimento.

Não Caia Nessa!

APRENDA A IDENTIFICAR GOLPES VIRTUAIS

Informação é a melhor proteção.

Compartilhe esta cartilha com sua família, seus amigos e, principalmente, com as pessoas mais velhas que você ama.

PARE · DESLIGUE · CONFIRME